Space-Efficient Side-channel Attack Resistant Table Lookups.

ABSTRACT OF THE INVENTION

Methods, apparatus and computer software and hardware products providing method, apparatus and system solutions for implementing table lookups in a side-channel attack resistant manner. Embodiments are provided for devices and situations where there is limited amount of RAM memory available or restrictions on memory addressing. The solutions solve problems associated with look up tables with large indices, as well as problems associated with looking up large sized tables or a collection of tables of large cumulative size, in limited devices, in an efficient side-channel attack resistant manner. These solutions provide defenses against both first-order side channel attacks as well as higher-order side channel attacks. One aspect of the present invention is the creation of one or more random tables which are used possibly in conjunction with other tables to perform a table lookup. This denies an adversary information about the table lookup from the side channel and thereby imparting side-channel resistance to the table lookup operation. Another aspect of the present invention is the use of a combination of some operations such as Table Split, Table Mask and Table Aggregate, to achieve this side-channel resistance within the limited amounts of available RAM and limited memory addressing capabilities of the device performing table lookups.